Controlled and Asymmetric Quantum Dialogue Protocol

Hongji Wang

School of Electronics & Information Engineering

Soochow University

Suzhou 215006, China

hongji\_wang@aliyun.com

Min Jiang

School of Electronics & Information Engineering

Soochow University

Suzhou 215006, China

jiangmin03@gmail.com

*Abstract*— Taking into account the asymmetric scenario that both Alice and Bob wish to communicate unequal amount of classical information, we propose an asymmetric quantum dialogue (QD) protocol based on the entanglement swapping between two-qubit bell state and four-qubit cluster state. In this scheme, assume that there are two legitimate participants Alice and Bob. In a dialogue, the information delivered by Alice to Bob is twice the amount of her information received from Bob. In addition, our protocol is extended to the controlled asymmetric quantum dialogue protocol, where one TP is responsible for the preparation of the initial state of the system, but also acts as a controller. We would like to point out that our scheme can work under the control of any number of controllers. Furthermore, our analysis demonstrates that our protocol is efficient and can fulfil the requirements of unequal amount of information transmission in a real communication scenario. Moreover, we discuss the security of this protocol and it demonstrates that our protocol could resist an external attack.

Keywords—asymmetric quantum dialogue, controlled asymmetric quantum dialogue, bell state, four-qubit cluster state, entanglement swapping

# Introduction

In recent years, more and more attention has been paid to quantum cryptography, which is developed to transmit classical and quantum information in a more efficient and safer manner.

As an important branch of quantum cryptography, quantum key distribution (QKD) [1][2][3] provides an absolutely secure communication method for two spatially separated communication users, whose security is guaranteed by the physical principles. Explicitly, both sides of communication are able to exchange secure information with the aid of sharing cryptography key in advance. BB84 is the first quantum key distribution protocol proposed by Bennett and Brassard in 1984, which encoded binary information by using four polarization states of single photon [] . Since then, although a large number of different QKD schemes have emerged, there have been still many constraints in the physical implementation of these schemes, such as the difficulty of photon detection, channel noise, etc. For the sake of addressing the problem that the realistic difficulty of photon detection limits the distance and speed of QKD, a practical approach is to construct quantum key distribution network, which is able to communicate between two no-adjacent users over long distances via intermediate forwarding nodes[ ]. Since then, besides QKD schemes, many other importation applications on quantum cryptography have been proposed, such as quantum secret sharing (QSS) [4-5], quantum teleportation [6-9], quantum secure direct communication (QSDC) [10-15] and so on.

As another important application in the field of quantum cryptography, quantum secure direct communication (QSDC) aims to allow two remote parties of communication can exchange secret information with each other directly without generating the private key to encrypt the secret information in advance. The biggest difference between quantum secure direct communication (QSDC) and QKD is whether or not the information is encrypted with a shared key before sending it. Since Beige et al. and long [ ]firstly presented the quantum secure direct communication scheme based on single-photon technology in 2002 [16][17], it has developed rapidly and evolved into an important branch of quantum information.

[Long, G.L., Liu, X.S., "Theoretically efficient high capacity quantum key distribution scheme", Physical Review A, 2002, 65(3):032302]

Various schemes with different quantum channels have been put forward. To elaborate further, Mi et al.[ ] proposed a encoding scheme based on the orbital angular momentum (OAM) states of photons with high information capacity and high security in 2015.

[Mi, S.C., Wang, T.J., Jin, G.S., et al., "High-Capacity Quantum Secure Direct Communication With Orbital Angular Momentum of Photons", IEEE Photonics Journal, 2015, 7(5)].

Give another example, the four requirements for constructing a real point-to-point QSDC network are proposed by Deng et al. [13]. Furthermore, they proposed two efficient QSDC network schemes with an N ordered EPR pairs. Based on this QSDC network scheme, any legitimate user can communicate safely and directly with another user.(逻辑和参考文献呢)

Taking into account the existence of the supervisor, another kind of quantum secure communication scheme with the controller named as CQSDC have been developed [10,18-20], where both sides of the communication can perform their one to one dialogue with the participation of controller. Afterwards, Hassanpour et al. proposed a CQSDC protocol based on GHZ-like state [20]. The analysis showed that the communication efficiency of their protocol has been greatly improved, and the scheme is absolutely secure because no qubits carrying private information are transmitted in the channel.

It should be pointed out that two remote users, Alice and Bob, can only transmit private information in one direction by using the QSDC or CQSDC schemes. To address this problem, Nguyen proposed the first bidirectional quantum secure direct communication (BQSDC) protocol for two parties exchanging their information simultaneously in 2004 [21]. Since then, BQSDC which is also called as quantum dialogue (QD) has become a hot topic in the field of academic research for the sake of allowing both remote legitimate parties to exchange their private information at the same time. In 2016, Wang et al. [25] proposed a quantum dialogue scheme with the four particle cluster state as the quantum channel, which also can satisfy the scenario of simultaneous communication between receiver and sender.

Anyhow，BQSDC still suffer one problem that needs to be taken seriously. That is, [in a real world scenario](http://ieeexplore.ieee.org/abstract/document/6612981/) the capacity of information communication between two users is not always identical. That is, the information amount from one party is different from another. However, in previous quantum dialogue protocols [22][23][24][25][26], the capacity of information transmitted between Alice and Bob always remains identical. Under such a circumstance, identical amount of two-way communication will enhance information redundancy which results in the large resource consumption and increases the burden of network.

To address the above problem, we propose an asymmetric quantum dialogue protocol, which is based on the entanglement swapping with two-qubit bell state and four-qubit cluster state. We analytically prove that the information that is delivered by Alice to Bob is twice the amount of her information received from Bob in a dialogue which leads to the reduction of qubits consumption. Furthermore, the detailed analysis demonstrates that our protocol is efficient and can ensure the efficient and secure transmission of quantum information.

The rest of this paper is organized as follows. In section 2, we first briefly illustrate some basic principles of entanglement swapping between two-qubit bell state and four-qubit cluster state and present the detailed procedure of our protocol. In section 3, we provide a detailed introduction on the controlled asymmetric quantum dialogue protocol. In section 4, the security is analyzed in detail. Subsequently, in section 5 we give a performance comparison between our schemes and others. Finally, we conclude our paper in section 6.

# Asymmetric Quantum Dialogue Protocol with Bell state and Four-Qubit Cluster State

## Preliminaries of entanglement swapping between two-qubit Bell state and four-qubit cluster state

Before delving into the presentation of our scheme, we introduce several important notations which will be used in our protocol.

Firstly, four Bell states are expressed as follows

(1-1)

(1-2)

(1-3)

. (1-4)

Secondly, four basic unitary transformations are expressed as: (2-1)

(2-2)

(2-3)

. (2-4)

Here, four unitary transformation and represent classic bits 00, 01, 10 and 11, respectively. It should be also noted that any Bell state can be converted with each other by performing one unitary operation labeled in Eqs (2.1)~(2.4) on any single qubit, i.e., the unitary operation is performed on the second qubit , as shown in the Table 1.

1. transformation relationship between any two Bell State

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |ψ0〉 | |ψ1〉 | |ψ2〉 | |ψ3〉 |
| |ψ0〉 |  |  |  |  |
| |ψ1〉 |  |  |  |  |
| |ψ2〉 |  |  |  |  |
| |ψ3〉 |  |  |  |  |

Thirdly, there are sixteen four-qubit cluster states composed of a set of orthogonal bases given by

|C〉1= (3-1)

|C〉2= (3-2)

|C〉3= (3-3)

|C〉4= (3-4)

|C〉5= (3-5)

|C〉6= (3-6)

|C〉7= (3-7)

|C〉8= (3-8)

|C〉9= (3-9)

|C〉10= (3-10)

|C〉11= (3-11)

|C〉12= (3-12)

|C〉13= (3-13)

|C〉14= (3-14)

|C〉15= (3-15)

|C〉16=. (3-16)

Explicitly, we note that a four-qubit cluster state can be converted into another cluster state if one of the unitary operations is applied to qubits 1, 2 and 4 of a four-qubit cluster state. In detail, the sixteen unitary operation are

(4-1)

(4-2)

(4-3)

(4-4)

(4-5)

(4-6)

(4-7)

(4-8)

(4-9)

(4-10)

(4-11)

(4-12)

(4-13)

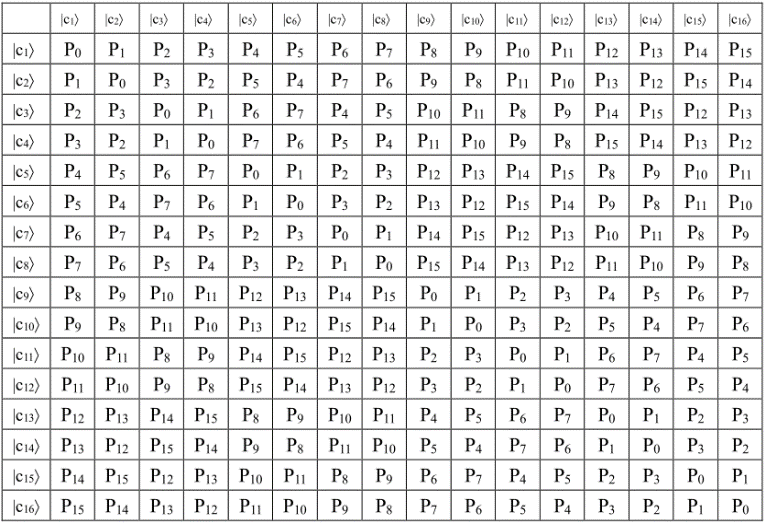
(4-14)

(4-15)

. (4-16)

Here ⊗ represents Kronecker product and Pi ( i = 0, 1, 2, …, 15 ) represent four bits of classical information 0000, 0001, …, 1111, respectively. The detailed relationship between any two four-qubit cluster state is shown in Table 2.

1. conversion relationship between any four-qubit Cluster state



Finally, we describe the principle of entanglement swapping between one two-qubit Bell state and one four-qubit cluster state. Fig.1 illustrates entanglement swapping between a two-qubit bell state and a four-qubit cluster state. It is shown that in the beginning the two systems were completely uncorrelated and the state of the whole system can be expressed as

(5)

With entanglement swapping, it can be rewritten as:

. (6)

where |C1〉CDEF=, |ψ0〉AB=.

In detail, when a joint measurement in the Bell basis is performed onto qubits B and E, then the state of the remaining qubits will be collapsed into another four-qubit cluster state. There are four possibilities of measurement outcomes {{}, {}, {}, {}}.



Fig.1 we note that a bell state consisting of qubit A and B is represented by two green circles, where the straight line between the two circles indicates that they are entangled. Similarly, qubit, C, D, E, and F constitute a cluster state, as denoted by four triangles. Consequently, this figure shows the entanglement swapping between two-qubit bell state and four-qubit cluster state.

Consider other three Bell states and fifteen four-qubit cluster states, we give all the left combinations. Here assume that

(7-1)

(7-2)

(7-3)

(7-4)

(7-5)

(7-6)

(7-7)

(7-8)

(7-9)

(7-10)

(7-11)

(7-12)

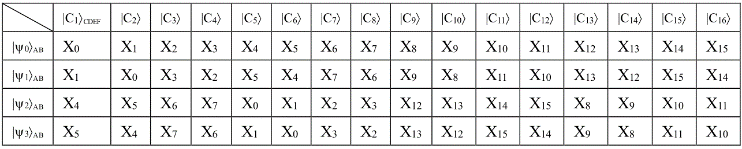
(7-13)

(7-14)

(7-15)

. (7-16)

1. In this way, a combinatorial list of entanglement swapping results for any Bell state and cluster state is concluded in Table 3.COMBINATORIAL LIST OF ENTANGLEMENT SWAPPING RESULTS FOR ANY BELL STATE AND CLUSTER STATE



# Controlled Asymmetric Quantum Dialogue Protocol

## Asymmetric quantum dialogue involving one controller

As mentioned in the introduction, two legitimate communication users cannot exchange secret information without the assistance of the controller, which has substantially increased the security of the quantum communication. Hence, we have to consider the asymmetric capacity quantum dialogue protocol that contains the controller for the sake of maximizing the security and flexibility of the quantum communication. In this context, let us consider the case shown in figure 2, where  TP is responsible for the preparation of the initial state of the system, but also acts as a controller.



Fig.2 This diagram shows the asymmetric quantum dialogue scheme with a controller, where TP is responsible for the preparation of the initial state of the system, but also acts as a controller.

Phase A: Preparing the quantum entangled states and checking the distribution security of the sharing qubits

Step 1: TP prepares one sequence of *N* entangled states, chosen randomly from four Bell states{(A1, B1), (A2, B2), …, (AN-1, BN-1) , (AN, BN)} and another sequence of *N* entangled states, chosen randomly in sixteen cluster states{(C1, D1, E1, F1), (C2, D2, E2, F2), …, (CN-1, DN-1, EN-1, FN-1) , (CN, DN, EN, FN)}. Furthermore, TP prepares two checking sequences P1 and P2 both of which are composed of N single qubits randomly in one of four states |0〉, |1〉, |+〉 and |-〉 for the sake of guaranteeing that each qubit can be safely distributed to both Alice and Bob.

Step 2: As mentioned at the beginning of this section, TP acts as a controller, which enhances the security of quantum communication between Alice and Bob by performing unitary operator on qubit Bn (n= 1, 2 , …, N). Hence, TP performs unitary operator On chosen randomly from Ui ( i = 1, 2, 3, 4 ) on qubit Bn, i.e. , { On(Bn)}, (n= 1, 2 , …, N). Additionally, TP divides the sequences into sixstrings and these strings can be denoted by: SA={ A1, A2, …, AN}, SB={ O1(B1), O2(B2), …, ON(BN)}, SC={C1, C2, …, CN}, SD={D1, D2, …, DN}, SE={E1, E2, …, EN}, SF={F1, F2, …, FN}.

Step 3: In our scenario, observe that the security of distributing qubits from TP to Alice and Bob can be undertaken with the aid of inserting checking qubits into the ordered sequences. Therefore, TP randomly inserts checking qubits of the sequences P1 and P2 into the ordered sequences SA and SE, respectively and gets two new sequences SA’’ and SE”. Subsequently, TP records their positions in the new sequences, and then sends the sequences SA’’, SC, SD, SF to Alice, and sends the sequences SB, SE” to Bob.

Step 4: To guarantee realization of the security checking process, both Alice and Bob must first confirm to TP that they have received all qubits of sequences SA’’, SC, SD, SF and sequences SB, SE”, respectively. In this context, Alice and Bob should collaborate to check the security of quantum channel with the following procedures: TP tells Alice and Bob the position of sample qubits of the sequences P1 and P2 in the detection sequence SA’’ and SE”, respectively. Subsequently, Alice and Bob select randomly corresponding bases BZ={|0〉, |1〉} or BX={|+〉, |-〉} to measure the sample qubits. Finishing measuring, for the sake of verifying as to whether the channel is secure, Alice and Bob compare their measurement results with the corresponding quantum state from TP’s announcements. In this context, Alice and Bob analyze the error rate. Explicitly, the quantum channel is insecure if the error rate exceeds the theoretical security threshold, then they terminate the communication.

Phase B: Encoding the secret information by performing the corresponding unitary operators

Step 1: Having verified the channel is secure, let us now proceed by elaborating on the details of phase B, where Alice and Bob encode their secret information by performing the corresponding unitary operators, respectively. Observe that in the step 3 of phase A TP randomly inserted checking qubits of the sequences P1 and P2 into the ordered sequences SA and SE, respectively. Hence, we note that Alice and Bob should remove the sample qubits from the sequences SA’’ and SE”, respectively, to restore the initial sequence SA and SE. Explicitly, Alice now holds the sequences SA, SC, SD and SF, and the sequences SB, SE belong to Bob.

Step 2: In the context of the previous step, let us consider the specific encoding process, which involves the execution of the corresponding unitary operators, where the unitary operators performed by Alice and Bob consisting of Pi ( i = 0, 1, 2, …, 15 ) and Ui ( i = 1, 2, 3, 4 ), respectively. In a nutshell, assume that Alice performs one of unitary operators Pi ( i = 0, 1, 2, …, 15 ) on qubits Cn, Dn and Fn, i.e. , { Pi(Cn Dn Fn) An }, (n= 1, 2 , …, N) to encode her 4n bits of secret information and Bob performs one of unitary operators Ui ( i = 1, 2, 3, 4 ) on qubit Bn, i.e. , { Ui(On(Bn)) En }, (n= 1, 2 , …, N) to encode his 2n bits of secret information.

Having provided a detailed description of the encoding process, let us now proceed by elaborating on the details of the implementation of decoding, where secret information can be delivered in both directions.

Phase C: Decoding the secret information

Step 1: In the context of achievement of the above encoding process, let us first consider the realization of the measurement, which performed by Alice and Bob, since it is capable of helping both Alice and Bob may exchange their secret information each other and simultaneously. Consequently, Alice measures { Pi(Cn , Dn ,Fn), An }, (n= 1, 2 , …, N) in four-qubit cluster basis defined as Eq (3) . Simultaneously, Bob measures { Ui(On(Bn)), En }, (n= 1, 2 , …, N) with the Bell basis. In this way, Alice can obtain one of the sixteen possible measurement outcomes and Bob can obtain one of four possible measurement outcomes. Then, the two legitimate users Alice and Bob publish their measurement results via classical channel.

Step 2: In our scenario, the quantum entanglement state before the encoding phase must be known for the sake of decoding the secret information. Due to this specific request, TP announces the preparation of the initial state defined by Eq. (9) and the unitary operators On that he has chosen randomly from Ui ( i = 1, 2, 3, 4 ) and performed on the qubit Bn (n= 1, 2 , …, N) of the bell states in step 2 of Phase A, where if he performs U1, U2, U3, or U4 on the qubits, he will publish “00”, “01”, “10”, or “11”, respectively.

(9)

In this context, the quantum entanglement state before the coding phase defined by Eq. (10) can be inferred by Alice and Bob with the aid of the aforementioned information announced by TP and the transformation relationship between any two bell states shown in Table 1.

(10)

Step 3: Having known the quantum entanglement state before the coding phase defined by Eq. (10), Alice(Bob) is able to deduce secret information that Bob(Alice) transmits to her(him) based on her(his) own unitary operation performed, both of their measurement results and table 3. In this way, both Alice and Bob may exchange their unequal amounts of information each other and simultaneously with the permission of the controller.

## Asymmetric quantum dialogue involving multiple controllers

Additionally, let us consider the case shown in figure 3, where there are multiple controllers in the scheme that serially control the asymmetric quantum dialogue between Alice and Bob. Let us now describe how these controllers (TP1~TPn) control the dialogue process between Alice and Bob.

We denote that TP1 is still responsible for the preparation of the initial state of the system. However, as for the qubit Bn (n= 1, 2 , …, N), they are no longer directly distributed to Bob, but rather TP1 performs unitary operator  chosen randomly from Ui ( i = 1, 2, 3, 4 ) on qubit Bn, i.e. , { (Bn) }, (n= 1, 2 , …, N), and then sends them to TP2. Subsequently, the TP2 as the second controller performs unitary operator  on qubit Bn , i.e. , { (Bn) }, (n= 1, 2 , …, N), and so on. Consequently, having performed the unitary operator on qubit Bn by the TPn, i.e. , {  (Bn) }, (n= 1, 2 , …, N), we note that the sequence SB can be denoted by SB={ (B1), (B2), …, (Bn)}, and then TPn sends it to Bob via quantum channel.

At this moment, we would like to point out that Alice and Bob cannot know the quantum entanglement state before the encoding phase without the assistance of n controllers. Consequently, for the sake of realizing the decoding process, TP1~TPn must inform their unitary operations to Alice and Bob via classical channel, respectively. Based on the aforementioned information published by n controllers, it is clear that Alice and Bob can achieve asymmetric quantum dialogue scheme with the aid of n controllers.



Fig.3 This figure shows the asymmetric quantum dialogue scheme involving multiple controllers, where TP1 is responsible for the preparation of the initial state of the system, but also acts as the first controller. Observe in this figure that TP1 ~ TPn need to perform the corresponding unitary operators for the sake of cotrolling the quantum dialogue with asymmetric capacity.

Having provided a brief description of our scheme through three phases, let us now proceed with a typical example of our proposed scheme for the sake of a better understanding of aforementioned steps that Alice can communicate with Bob by the permission of two controllers.

For the sake of simplicity, assume that the initial quantum entanglement state of qubits A and B is and the state of qubits C, D, E and F is. After the above quantum entanglement states are prepared by TP1, TP1 performs unitary operator = U2 on qubit B, i.e. , { U2(B)} for the sake of acting as the first controller, and then sends it to TP2. Subsequently, TP2 as the second controller performs unitary operator = U1 on qubit B, i.e. , { U1U2(B)}, and then sends it to Bob. Based on the above operation, the preparation of the initial state defined by Eq. (11) was converted to the pre-coding quantum entanglement state defined by Eq. (12), since the bell state was converted to with the unitary operator = U1U2 performed on qubit B by TP1 and TP2 (controller1 and controller2).

(11)

(12)

Explicitly, we do not have to consider all the sending possibilities, instead, we only assume that Alice’s and Bob’s secret information are “0001” and “01”, respectively. Consequently, Alice will perform unitary operation P1=U1⊗ U1 ⊗U2 on qubits C, D and F to encode her classical information 0001, while Bob performs unitary operation U2 on qubit B to encode his classical information 01. At this point, the cluster state |C1〉CDEF and Bell state will be transferred to |C2〉CDEF and |ψ0〉AB. The relationship of entanglement swapping is as follows

(13)

Having achieving the above encoding process, TP1 announced the preparation of the initial state defined by Eq. (11) and the unitary operation , while TP2 announced the unitary operation for the sake of assisting Alice and Bob to deduce the pre-coding quantum entanglement state. According the above information and the table.1, Alice and Bob are able to deduce the pre-coding quantum entanglement state defined by Eq. (12).

Subsequently, Alice measures her qubits C, D, F, A with the four-qubit cluster basis and Bob measures his qubits B, E with the Bell basis. Then they release their measurement outcomes with each other. If the measurement result set is X1 i.e., according to the Table.3, since Alice know the transformed state |C2〉CDEF, she can deduce that Bob’s transferred Bell state is |ψ0〉AB. Based on the Bell state , which stems from with the unitary operator = U1U2 performed on qubit B by TP1 and TP2, she can encoded information from Bob is 01. At the same time, based on the entanglement measurement result and his operation, Bob can deduce that Alice’s transferred cluster state is |C2〉CDEF and encoded information from Alice is 0001. In this way, Alice and Bob are able to complete quantum dialogue with asymmetric capacity by the permission of two controllers.

# Security Analysis of the Protocol

The advantage of our protocol is twofold: on the one hand, it can be applied to the scene that the two legitimate communication parties exchange unequal amount of secret information, where the information that is delivered by Alice to Bob is twice the amount of her information obtained from Bob in a dialogue.

On the other hand, there is no risk of information leakage in our protocol. Naturally, this is justified by the fact that a quantum dialogue protocol with superior performance should ensure that the secret information must be only available to the two legitimate users of the communication [29]. Observe in the implementation process of the protocol that the security problems in the proposed protocol mainly come from the transmission of quantum states in quantum channels. Additionally, we note that there may be two other types of attacks, namely the denial of service attack and TP is dishonest attack, which exist in the controlled asymmetric quantum dialogue protocol represented in section 3. Consequently, let us analyze in detail the impact of these attacks on our scheme.

## Intercept-Resend Attack

Even if the outsider attacker Eve intercepted the qubit sequences sent by Alice to Bob and the initial states of the preparation of the sequences, he is also unable to obtain any secret information of Alice and Bob. To elaborate further, let us consider this case, where Eve intercepts some qubits of the sequence SB’’ and the SE’’ when Alice sends to Bob, then sends a prepared sequence composed of fake qubits to Bob. However since the fake qubits prepared by Eve are randomly placed in one of the four states {|0〉, |1〉, |+〉, |-〉} and the initial entanglement correlation between the example qubits has been disturbed, the error rate will exceed the threshold when Bob announces his measurement results and measuring basis [22]. In this case, it is clear that both of them realize that the quantum channel is insecure and will terminate their communication.

## Entanglement-and-Measure Attack

For the sake of elaborating this attack, assume that the attacker Eve has prepared two sequences S1, S2 composed of auxiliary qubits and each initial state of the auxiliary qubits is |0〉. Subsequently, Eve has entangled the qubits of the sequences S1 and the S2 with the qubits of the sequences SB’’ and the SE’’ when Alice sends to Bob, respectively. In this context, the analysis shows that Eve and Bob can get the same state by performing controlled-not (CNOT) operation with the qubits S1 and the S2 are target qubits and the qubits SB’’ and the SE’’ are controller qubits, respectively.

However, observe that Alice prepares two checking sequences P1 and P2 both of which are composed of N single qubits randomly in one of four states |0〉, |1〉, |+〉, |-〉. Consequently, we note that the error rate will exceed the threshold when Alice and Bob collaborate to detect channel security if Eve launched an Entanglement-and-Measure attack.

## The Denial of Service Attack

In the context of this attack, we note that the attacker Eve gets the distribution sequences of TP sends to Alice and Bob, and then transmits his fake qubits to them for the sake of stealing the secret information from two legitimate users. In fact, the attack strategy is the same as the intercept-resend attack in the asymmetric quantum dialogue protocol without controller. Explicitly, we note that the security of the distribution sequences is well guaranteed with the aid of the checking sequences P1 and P2. Hence, the attack will be perfectly prevented by Alice and Bob jointly detecting the correlation of the distribution qubits.

## The TP Is Dishonest

In section 3, we proposed an enhanced version of asymmetric quantum dialogue protocol with a controller, namely controlled asymmetric quantum dialogue protocol, where TP is responsible for the preparation of the initial state of the system, but also acts as a controller. In this context, let us consider the case, where TP is dishonest. Despite the fact that the measurement results published by Alice and Bob, he cannot get the secret information exchanged between Alice and Bob, since the unitary operations of encoding the secret information performed by Alice and Bob are not published. Based on the above analysis, we note that there is no information leaked to anyone other than two legitimate users.

Having discussed the above four possible attacks, we may now conclude that the security of quantum channels has been guaranteed in the proposed protocol, regardless of whether containing a controller.

# performance comparison

Ideally we hope that the efficiency of communication can be 100%, explicitly, we note that this is not possible in practical scenarios, since the reliability of communication is usually guaranteed with the aid of adding extra redundancy information. For this reason, this is justified by the fact that taking into account the reliability and efficiency can make the scheme more practical. Based on the above ideas, we proposed two efficient protocols, namely asymmetric quantum dialogue protocol and controlled asymmetric quantum dialogue protocol, which are described in detail in the previous section of this paper.

Before delving into the performance comparison, we provided a definition of the efficiency of quantum communication, which is defined as

(14)

where bs denotes the number of secret information transmitted, qt and bt correspond to the qubits used and classical bits exchanged between Alice and Bob.

In this context, let us consider the comparison of our schemes with the others like Chou et al. [30], Li et al. [31] and Zarmehi et al. [10] which will be shown as Table 4. To elaborate further, observe in table 4 that the efficiency of our scheme is significantly higher regardless of whether it contains the controller.

1. Comparison of our schemes with the others

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scheme | Chou2014 | Li2013 | Zarmehi2016 | Ours |
| Type | CBQSDC | CBQSDC | CBQSDC | CAQD |
| bs | 2 | 2 | 8 | 6 |
| qt | 7 | 6 | 8 | 6 |
| bt | 5 | 6 | 12 | 6 |
| η(%) | 16.67 | 16.67 | 40 | 50 |

CAQD=Controlled Asymmetric Quantum Dialogue

# Conclusion

In summary, we have proposed a quantum dialogue scheme, namely controlled and asymmetric quantum dialogue protocol, which is realized by using the entanglement swapping between any two-qubit bell state and any four-qubit cluster state. Furthermore, we note that TP is responsible for the preparation of the initial state of the system, but also acts as a controller. Subsequently, for the sake of maximizing the security and flexibility of the quantum communication, we considered the case, where the asymmetric quantum dialogue protocol is controlled by multiple controllers. In our protocol, we note that the information that is delivered by Alice to Bob is twice the amount of her information obtained from Bob in a dialogue. In other words, this quantum communication scheme is a good solution to the problem that most of the quantum dialogue protocols must exchange the same amount of information between Alice and Bob that always brings information redundancy. In our controlled and asymmetric quantum dialogue protocol, the redundant information between Alice and Bob is extremely little because our protocol allows that the two legitimate communication parties can exchange unequal amount of secret information. Moreover, the analysis demonstrates that the protocol does not exist the problem of information leakage and can resist external attacks.

##### Acknowledgments

This work is supported by the National Natural Science Foundation under Grant No. 61473199 and No. 61104002.

##### References

1. Lo, H.K., Chau, H.F., "Unconditional security of quantum key distribution over arbitrary long distances", Science, 1999, 283(5410):2050
2. Vazirani, U., Vidick, T., "Fully device-independent quantum key distribution", Physical Review Letters, 2014, 113(14):140501
3. Nielson, M.A., Chuang, I.L., "Quantum Computation and Quantum Information", Cambridge University Press, United Kingdom, 10th Anniversary Edition, 2010
4. Du, R., Wang, B., Long, D., "Quantum Secret Sharing of Secure Direct Communication Using One-Time Pad", Internation Journal of Theoretical Physics, 2012, 51(9):2727-2736
5. Chen, X.B., Niu, X.X., Zhou, X.J., et al., "Multi-party quantum secret sharing with the single-particle quantum state to encode the information", Quantum Information Processing, 2013, 12(1):365-380
6. Bennett, C., Brassard, G., Crepeau, C., et al., "Teleproting an unknown quantum state via dual classical and EPR channels", Physical Review Letters, 1993, 70(13):1895
7. Jiang, M., Huang, X., Zhou, L.L., et al., "Quantum state transformation and general design scheme on teleportation protocols", Chinese Science Bulletin, 2012, 57(18):2247-2251
8. Oh, S., Lee, S., Lee, H.W., "Fidelity of Quantum Teleportation through Noisy Channels", Physical Review A, 2002, 66(2):207-212
9. Marzalino, U., Buchleitner, A., "Quantum teleportation with identical particles", Physical Review A, 2015, 91(3)
10. Zarmehi, F., Houshmand, M., "Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement", IEEE Communications Letters, 2016, 20(10):2071-2074
11. Yang, C.W., Hwang, T., "Improved QSDC Protocol over a Collective-Dephasing Noise Channel", International Journal of Theoretical Physics, 2012, 51(12):3941-3950
12. Jin, X.R., Ji, X., Zhang, Y.Q., et al., "Three-party quantum secure direct communication based on GHZ states", Physics Letters A, 2006, 354(1-2):67-70
13. Deng, F.G., Li, X.H., Li, C.Y., et al., "Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs", Physics Letters A, 2006, 359(5):359-365
14. Wang, S.A., Lu, C.Y., "Quantum secure direct communication network", Nanotechnology, IEEE, 2014:752-755
15. Gao, F., Qin, S.J., Wen, Q.Y., et al., "Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state", Optics Communications, 2010, 283(1):192-195
16. Beige, A., Englert, B.G., Kurtsiefer, C., Weinfuter, H.: Secure communication with a publicly known key. Acta Phys. Pol. A 101(3), 357(2002)
17. Zhou, NR., Wu, GT., Gong, LH. et al.: Secure Quantum Dialogue Protocol Based on W States Without Information Leakage. Int J Theor Phys. 52(9), 3204-3211(2013)
18. Chen, X.B., Wen, Q.Y., Guo, F.Z., et al., "controlled quantum secure direct communication with W state", International Journal of Quantum Information, 2008, 6(04)
19. Patwardhan S., Moulick, S.R., Panigrahi, P.K., "Efficient Controlled Quantum Secure Direct Communication Protocols", Internatioanal Journal of Theoretical Physics", 2016, 55(7):3280-3288
20. Hassanpour, S., Houshmand, M., "Efficient controlled quantum secure direct communication based on GHZ-like states", Quantum Information Processing, 2015, 14(2):739-753
21. Nguyen, B.A.: Quantum dialogue. Phys. Lett. A. 328(1), 6(2004)
22. Gao, G.: Two quantum dialogue protocols without information leakage. Opt. Commun. 283(10), 2288-1193(2010)
23. Wang, M., Ma, W., Shen, D. et al.: A Quantum Dialogue Protocol Based on Four-Qubit Entangled State. Int J Theor Phys. 54(4), 1388-1395(2015)
24. Yin, AH., Tang, ZH.: Two-Step Efficient Quantum Dialogue with Three-Particle Entangled W State. Int J Theor Phys. 53(8), 2765-2767(2014)
25. Wang, R., Li, D., Liu, Y. et al.: Two Ways of Robust Quantum Dialogue by Using Four-Qubit Cluster State. Int J Theor Phys. 55(4), 2110-2124(2016)
26. Zhang, Q., Li, C., Li, Y. et al.: Quantum Secure Direct Communication Based on Four-Qubit Cluster States. Int J Theor Phys. 52(1), 22-26(2013)
27. Zhan, YB., Zhang, LL., Wang, YW., et al.: Quantum Dialogue by Using Non-Symmetric Quantum Channel. Communications in Theoretical Physics. 53(4), 648(2010)
28. Banerjee, A., Shukla, C., Thapliyal, K. et al.: Asymmetric Quantum Dialogue in Noisy Environment. Quantum Inf Process. 1-2(2017)
29. Li, J., Jin, HF., Jing, B.: Improved eavesdropping detection strategy based on four-particle cluster state in quantum direct communication protocol. Sci. Bull. 57(34), 4434(2012)
30. Chou, Y.H., Lin, Y.T., Zeng, G.J., et al., "Controlled bidirectional quantum secure direct communication", The Scientific World Journal, 2014, 2014(6):694798
31. Li, Y.H., Li, X.L., Sang, M.H., et al., "Bidirectional controlled quantum teleportation and secure direct communication using five-qubit entangled state", 2013, 12(12):3835-3844